

ЗАТВЕРДЖЕНО  
ЄААД.468244.185-ЛУ

Підп. та дата	
Інв. № дубл	
Взам. інв. №	
Підп. та дата	
Інв. № ориг.	

**Центр сертифікації ключів  
ринку електричної енергії**

**Комплексна система захисту інформації**

**Модель загроз безпеки інформації**

ЄААД.468244.185.Д2.02

**ЗМІСТ**

ПЕРЕЛІК СКОРОЧЕНЬ .....	3
ТЕРМІНИ ТА ВИЗНАЧЕННЯ.....	3
1 ЗАГАЛЬНІ ПОЛОЖЕННЯ.....	4
2 СТИСЛА ХАРАКТЕРИСТИКА ЦСК І ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ .....	5
3 ЗАГРОЗИ ДЛЯ ІНФОРМАЦІЇ, ЯКА ОБРОБЛЯЄТЬСЯ В ЦСК .....	6
4 МОДЕЛЬ ПОРУШНИКА.....	11
5 ПЕРЕЛІК СУТТЄВИХ ЗАГРОЗ В ЦСК .....	18
6 СПОСОБИ ЗДІЙСНЕННЯ ЗАГРОЗ .....	20
7 ОЦІНКА ПЕРЕДБАЧУВАНОВОГО ЗБИТКУ У РАЗІ РЕАЛІЗАЦІЇ ЗАГРОЗ .....	21
8 ШЛЯХИ РЕАЛІЗАЦІЇ ОСНОВНИХ ЗАГРОЗ ТА СПОСОБИ ЇХ НЕЙТРАЛІЗАЦІЇ.....	22
9 ВИСНОВКИ .....	27

### ПЕРЕЛІК СКОРОЧЕНЬ

БД	- База даних
ДСТУ	- Державний стандарт України
ДТЗС	- Допоміжні технічні засоби та системи
ЕЦП	- Електронний цифровий підпис
ІзОД	- Інформація з обмеженим доступом
КЗЗ	- Комплекс засобів захисту
КНОІ	- Канал несанкціонованого отримання інформації
КСЗІ	- Комплексна система захисту інформації
НД	- Нормативний документ
НСД	- Несанкціонований доступ
ПЗ	- Програмне забезпечення
ОЗП	- Оперативний запам'ятовуючий пристрій
ОТЗ	- Основні технічні засоби
РС	- Робоча станція
СЗІ	- Служба захисту інформації
ТЗІ	- Технічний захист інформації
ТЗ СЕВ	- Технічні засоби силового електромагнітного впливу
ЦСК	- Центр сертифікації ключів

### ТЕРМІНИ ТА ВИЗНАЧЕННЯ

У цьому документі використовуються терміни та визначення згідно з:

- ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення";
- НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

## 1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1 Створюваний ЦСК є інформаційно-телекомунікаційною системою. Згідно Законів України “Про інформацію”, “Про захист інформації в інформаційно-телекомунікаційних системах”, а також НД ТЗІ 1.4-001-2000 в ЦСК має бути розроблена та створена комплексна система захисту інформації (далі - КСЗІ).

1.2 Порядок розробки і створення КСЗІ в ЦСК регламентується комплексом нормативно-правових документів в області технічного і криптографічного захисту інформації, перелік яких визначений Адміністрацією Держспецзв'язку України.

1.3 Модель загроз розроблена з урахуванням вихідних даних, що містяться в матеріалах обстеження ЦСК, відповідно до вимог:

- ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;
- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;
- ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення;
- НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБ України від 28.04.99 р. № 22;
- НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ від 28 квітня 1999 року №22;
- НД ТЗІ 1.1-002-98. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ від 28 квітня 1999 року №22;
- НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджений наказом ДСТСЗІ СБУ №37 від 18.06.2002 р.;
- НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджений наказом ДСТСЗІ СБУ від 13.12.2002 р. №84;
- НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджений наказом ДСТСЗІ СБУ від 4 грудня 2000 року №53;
- Правила посиленої сертифікації. Затверджені наказом ДСТСЗІ СБ України № 50 від 10.05.2006 р.;
- накази та розпорядження ДП “ЕНЕРГОРИНОК”.

1.4 Модель загроз ЦСК розроблена за результатами:

- аналізу архітектури і класифікації ресурсів ЦСК та його складових частин;
- аналізу неформальної моделі можливих інформаційних потоків у функціональних підсистемах, складових частинах і ЦСК в цілому;
- визначення і аналізу інформаційних ресурсів складових частин і ЦСК в цілому, підлягаючих захисту (об'єктів захисту);
- визначення переліку загроз і можливих каналів витоку інформації з оцінкою можливих втрат у разі здійснення загроз.

1.5 Дана модель визначає склад і джерела загроз, оцінку можливості їх прояву, шляхи їх здійснення, оцінку очікуваного збитку від реалізації загроз.

1.6 Модель загроз ЦСК призначена для аналізу ризиків, визначення політики безпеки інформації і вимог до КСЗІ ЦСК, формування планів технічного захисту інформації (ТЗІ), реалізації організаційних, первинних і основних технічних заходів захисту ІзОД і контролю функціонування КСЗІ ЦСК.

## **2 СТИСЛА ХАРАКТЕРИСТИКА ЦСК І ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ**

2.1 Стисла характеристика ЦСК і технології обробки інформації наведені в дод. 2 до плану захисту інформації в ЦСК.

### 3 ЗАГРОЗИ ДЛЯ ІНФОРМАЦІЇ, ЯКА ОБРОБЛЯЄТЬСЯ В ЦСК

3.1 Наявність інформаційних зв'язків з інформаційними системами інших організацій та відомств, використання національних і корпоративних систем передачі, що знаходяться під управлінням інших операторів, і надання послуг користувачам, які не є співробітниками ЦСК, створюють передумови виникнення загроз для інформації і ресурсів ЦСК.

3.2 Загрози для інформації, яка обробляється в складових частинах та пересилається по каналах передачі даних, залежать від характеристик обчислювальної системи, фізичного середовища, персоналу, технологій обробки і оброблюваної інформації ЦСК. Загрози можуть мати об'єктивну або суб'єктивну природу. Загрози, які мають суб'єктивну природу, можуть бути випадковими (ненавмисними) або навмисними.

3.3 Для компонентів локальної обчислювальної мережі (ЛОМ) та зовнішніх каналів передачі даних ЦСК потенційно можливими джерелами загроз об'єктивної природи можуть бути:

- випадкові зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту), такі як стихійні лиха і аварії, землетрус, повінь, пожежа або інші випадкові події;
- випадкові зміни умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони) такі, як аварія системи електропостачання приміщень будівлі, руйнування будівельних конструкцій приміщень будівлі, затоплення приміщень унаслідок аварії інженерних комунікацій холодного водопостачання та опалення, пожежа та інші випадкові події;
- випадкові збої і відмови в роботі оснащення і технічних засобів компонентів ЦСК.

3.4 Потенційно можливими джерелами загроз суб'єктивної природи можуть бути:

- навмисні зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту), такі як впливи (аварії, пожежа або інші навмисні події) на комутаційні вузли і канали (тракти) передачі первинної мережі зв'язку і т. ін.) ;
- зміна умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони), такі як аварія системи електропостачання приміщень будівлі, руйнування будівельних конструкцій приміщень будівлі, затоплення приміщень унаслідок аварії інженерних комунікацій холодного водопостачання та опалення, пожежа або інші випадкові події;
- наслідки помилок під час проектування і розробки компонентів ЦСК (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних та ін.);
- помилки персоналу (користувачів) ЦСК під час експлуатації обладнання і технічних засобів компонентів ЦСК;
- навмисні дії (спроби) потенційних порушників під час експлуатації обладнання і технічних засобів компонентів ЦСК.

3.5 Джерелами навмисних пасивних і активних загроз у відношенні ЦСК можуть бути внутрішні (нелояльні співробітники) і зовнішні (користувачі ЦСК і т.ін.). Джерела виникнення загроз щодо складових частин ЦСК групуються на класи. У свою чергу кожний клас загроз включає сукупності загроз, що згруповані по каналах реалізації.

Системна класифікація загроз ЦСК виконана за наступними критеріями:

а) по місцю знаходження інформації і ресурсів щодо процесу автоматизованої обробки:

- загрози можуть виявитися незалежно від обробки, тобто обумовлені самим фактом існування ЦСК;
- загрози, що проявляються тільки в процесі безпосередньої обробки інформації;

б) по положенню джерел загроз щодо компонентів ЦСК і їх взаємодії з компонентами:

- зовнішні джерела загроз, тобто джерела загроз знаходяться за межами складових частин ЦСК;
- внутрішні джерела загроз, тобто джерела загроз знаходяться в межах складових частин ЦСК;

в) по взаємодії джерел загроз з компонентами ЦСК:

- без змін в компонентах складових частин ЦСК;
- з випадковим або навмисним внесенням змін в технічні засоби, програми, бази даних і т.ін.

3.6 Поєднання значень обраних критеріїв утворюють множину з шести варіантів, кожний з яких є класом однорідних за певними ознаками загроз інформації в ЦСК. Класи загроз інформації в ЦСК наведені в табл. 1.

Таблиця 1 - Класи загроз інформації в ЦСК

Положення джерела загроз		Положення інформації, що захищається	
		не залежить від обробки	проявляється при обробці
Поза межами ЦСК і його складових частин		1 клас	2 клас
В межах ЦСК і його складових частин	Без зміни компонентів ЦСК	3 клас	4 клас
	Зі зміною компонентів ЦСК	5 клас	6 клас

3.7 В табл. 2 наведена структура і перелік суттєвих загроз (каналів несанкціонованого отримання інформації, КНОІ) за класами загроз. Під КНОІ розуміються такі можливі способи здійснення загроз, наслідком яких може бути отримання (або небезпека отримання) інформації, що захищається, особами або процесами, що не мають на це повноважень.

Таблиця 2. Структура і перелік каналів несанкціонованого отримання інформації

Клас КНОІ	Фактори, наслідком яких може бути отримання (або небезпека отримання) інформації, що захищається, особами або процесами, які не мають на це повноважень.
КНОІ 1-го класу - канали виявляються безвідносно до обробки інформації і без доступу порушника до елементів складових частин ЦСК.	помилки і системні неузгодженості при проектуванні архітектури системи, технології обробки інформації, розробці прикладних програм; розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток і т. п.); розкрадання носіїв інформації з місць зберігання; підслуховування розмов осіб, що мають відношення до рішення тематичних задач ЦСК; провокація на розмови осіб, які мають відношення до рішення тематичних задач ЦСК; використання порушником візуальних засобів; використання порушником оптичних засобів; використання порушником акустичних засобів.
КНОІ 2-го класу - канали виявляються в процесі обробки інформації без доступу порушника до елементів складових частин ЦСК.	збої і помилки в роботі апаратно-програмних засобів в процесі обробки ІзОД; помилки в програмах обробки ІзОД, які можуть привести до витоку інформації; передача даних за помилковою адресою абонента (помилкова зміна маршруту); перехоплення інформації в лініях (каналах) зв'язку мережі загального користування шляхом підключення; електромагнітні випромінювання пристроїв наглядного відображення; побічні електромагнітні випромінювання технічних засобів обробки ІзОД; електромагнітні випромінювання ліній зв'язку; електромагнітні випромінювання допоміжної апаратури; паразитні наведення в комунікаціях водопостачання; паразитні наведення в мережі теплопостачання; паразитні наведення в системах вентиляції; паразитні наведення в шинах заземлення; паразитні наведення в ланцюгах часофікації; паразитні наведення в ланцюгах радіофікації; паразитні наведення в ланцюгах телефонізації; паразитні наведення в мережах живлення; підключення генераторів ВЧ-нав'язування; підключення апаратури реєстрації;
КНОІ 3-го класу - канали виявляються безвідносно до	копіювання бланків з вихідними даними; копіювання магнітних носіїв;

обробки інформації з доступом порушника до елементів складових частин ЦСК, але без зміни останніх.	копіювання з пристроїв відображення; копіювання вихідних документів; копіювання інших документів; розкрадання виробничих відходів; підкуп, шантаж користувачів, які працюють з ІзОД
КНОІ 4-го класу - канали, що виявляються в процесі обробки інформації з доступом порушника до елементів складових частин ЦСК, але без зміни останніх.	запам'ятовування інформації на бланках з вихідним даними; запам'ятовування інформації з пристроїв відображення; запам'ятовування інформації на вихідних документах; запам'ятовування службових даних; копіювання (фотографування) інформації з пристроїв відображення в процесі обробки; вхід в систему в обхід засобів захисту; читання залишкової інформації з оперативної пам'яті і зовнішніх запам'ятовуючих пристроїв; використання програмних «пасток»; маскування під зареєстрованого користувача; використання недоліків мов програмування; використання недоліків операційних систем; використання зараження програмного забезпечення «вірусом»; несанкціонована зміна особистих повноважень або повноважень інших користувачів на відправлення і отримання повідомлень; маскування під зареєстрованого користувача або запити системи; видача одного об'єкту за іншого з метою використання його повноважень для формування помилкової інформації або команд управління; видача одного об'єкту або суб'єкта за іншого для того, щоб зняти з себе відповідальність за реалізовані або спроби реалізувати певні загрози; санкціонування помилкових обмінів повідомленнями або їх підтвердження;
КНОІ 5-го класу - канали, що виявляються безвідносно до обробки інформації з доступом порушника до елементів складових частин ЦСК зі зміною останніх.	підміна бланків, магнітних носіїв, вихідних документів, елементів програм, елементів баз даних; розкрадання бланків з вихідним даними, магнітних носіїв, вихідних документів, інших документів; несанкціонований доступ (використання) до пристрою і інформаційно-програмного забезпечення (у тому числі базам даних); зміна режимів технічних засобів або програм; впровадження і використання несанкціонованого програмного забезпечення; некомпетентне використання, настройка або неправомірне відключення засобів захисту персоналом служб захисту; впровадження апаратних і програмних «закладок» і «вірусів»; зчитування залишкової інформації в ОЗП після виконання санкціонованих запитів.
КНОІ 6-го класу - канали, що виявляються в процесі обробки інформації з доступом порушника до елементів складових частин ЦСК зі зміною останніх.	незаконне підключення до апаратури; несанкціонований доступ (підключення, зміна) до пристроїв і інформаційно-програмного забезпечення (у тому числі базам даних); незаконне підключення до ліній зв'язку; зняття інформації на шинах живлення пристроїв наглядного відображення; зняття інформації на шинах живлення процесорів; зняття інформації на шинах живлення апаратури зв'язку; зняття інформації на шинах живлення друкуємих пристроїв; зняття інформації на шинах живлення апаратури ліній зв'язку; зняття інформації на шинах живлення зовнішніх запам'ятовуючих пристроїв; зняття інформації на шинах живлення допоміжної апаратури; отримання атрибутів доступу в ЛОМ з наступним їх



	використанням для маскуванню під зареєстрованого користувача ("маскарад"); впровадження і застосування ПЗ забороненого політикою безпеки або несанкціоноване використання ПЗ, за допомогою якого можна отримати доступ до критичної інформації (наприклад, аналізаторів безпеки мережі).
--	---

### 3.8 Вплив загроз інформаційної безпеки на властивості інформації і ЦСК

3.8.1 В табл. 3 наведені структура і перелік каналів потенційно можливих причин несанкціонованого порушення цілісності або доступності інформації (КНЦД) по класах загроз. Під КНЦД розуміються такі можливі способи здійснення загроз, наслідком прояву яких може бути порушення особами або процесами, що не мають на це повноважень, фізичної і логічної цілісності або доступності інформації.

Таблиця 3 - Структура і перелік каналів потенційно можливих причин несанкціонованого порушення цілісності або доступності інформації

Клас КНЦД	Фактори, наслідком прояву яких може бути порушення особами або процесами, що не мають на це повноважень, фізичної і логічної цілісності або доступності інформації
КНЦД 1-го класу - канали виявляються безвідносно до обробки інформації і без доступу порушника до елементів складових частин ЦСК.	випадкове або навмисне знищення носіїв інформації в місцях зберігання; випадкові зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту) такі як: стихійні лиха і аварії, землетрус, повінь, пожежа або інші випадкові події; випадкові зміни умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони) такі як: аварія системи електропостачання приміщень будівлі, руйнування будівельних конструкцій приміщень будівлі, затоплення приміщень внаслідок аварії інженерних комунікацій холодного водопостачання, опалювання, пожежа або інші випадкові події; випадкові збої (неправильне виконання функцій) і відмови (повний вихід з ладу) в роботі обладнання і технічних засобів компонентів ЦСК; відмови та збої носіїв інформації; невиконання вимог до організаційних заходів захисту діючих в ЦСК розпорядчих документів.
КНЦД 2-го класу - канали виявляються в процесі обробки інформації без доступу порушника до елементів складових частин ЦСК;	підключення генераторів перешкод; знищення носіїв інформації в місцях зберігання; випадкові зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту) такі як: стихійні лиха і аварії, землетрус, повінь, пожежа або інші випадкові події; випадкові або навмисні зміни умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони) такі як: аварія системи електропостачання приміщень будівлі, руйнування будівельних конструкцій приміщень будівлі, затоплення приміщень внаслідок аварії інженерних комунікацій холодного водопостачання, опалювання, пожежа або інші випадкові події; випадкові збої і відмови в роботі обладнання і технічних засобів компонентів ЦСК; відмови і збої носіїв інформації; невиконання вимог до організаційних заходів захисту діючих в ЦСК розпорядчих документів.
КНЦД 3-го класу канали виявляються безвідносно до обробки інформації з доступом порушника до елементів складових частин ЦСК, але без зміни останніх.	неправомірною зміною режимів роботи елементів складових частин ЦСК (окремих компонентів, обладнання, ПЗ та ін.); запуск тестових або технологічних процесів, які здатні привести до незворотних змін в системі (наприклад, форматування носіїв інформації); випадкові збої і відмови в роботі оснащення і технічних засобів компонентів ЦСК; невиконання вимог до організаційних заходів захисту діючих в ЦСК розпорядчих документів; наслідки некомпетентного застосування засобів захисту.
КНЦД 4-го класу - канали,	неправомірною зміною режимів роботи елементів складових частин

<p>що виявляються в процесі обробки інформації з доступом порушника до елементів складових частин ЦСК, але без зміни останніх.</p>	<p>(окремих компонентів, обладнання, ПЗ та ін.); запуск тестових або технологічних процесів, які здатні привести до незворотних змін в системі (наприклад, форматування носіїв інформації; випадкові збої і відмови в роботі обладнання і технічних засобів компонентів ЦСК; невиконання вимог до організаційних заходів захисту діючих в ЦСК розпорядчих документів; помилки під час введення даних в систему, виведення даних за помилковими адресами пристроїв, внутрішніх і зовнішніх абонентів та ін.; неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, учбові і ігрові програми, системне і прикладне забезпечення та ін.); наслідки некомпетентного застосування засобів захисту; відмова одержувача (відправника) від факту прийому (передачі) інформації або твердження, що вона прийнята (передана) в інший час; формування одержувачем помилкової інформації, нібито отриманої від відправника; твердження про те, що повідомлення або запит передавалися, хоча насправді вони не передавалися або передавалися в інший час; твердження про те, що повідомлення або запит отримано від певного користувача, хоча насправді вони сформовані одержувачем (порушником); навмисна зміна одержувачем повідомлень з метою порушення їх цілісності і автентичності; формування відправником помилкового підтвердження отримання інформації, нібито прийнятого від одержувача.</p>
<p>КНЦД 5-го класу - канали, що виявляються безвідносно до обробки інформації з доступом порушника до елементів складових частин ЦСК зі зміною останніх.</p>	<p>випадкові збої і відмови в роботі обладнання і технічних засобів компонентів ЦСК; ненавмисне зараження "вірусами"; невиконання вимог до організаційних заходів захисту діючих в ЦСК розпорядчих документів; помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів та ін.; неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, учбові і ігрові програми, системне і прикладне забезпечення та ін.); наслідки некомпетентного застосування засобів захисту; включення в програми модулів типу "троянський кінь", "бомба" та ін.; видача одного об'єкту або суб'єкта за іншого, для того, щоб зняти з себе відповідальність за реалізовані або спроби реалізувати певні загрози.</p>
<p>КНЦД 6- го класу - канали, що виявляються в процесі обробки інформації з доступом порушника до елементів складових частин ЦСК із зміною останніх.</p>	<p>пошкодження апаратури, програм, елементів баз даних, носіїв даних, вихідних документів; дії, які приводять до відмови окремих компонентів ЦСК, порушення апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, віддалення даних, програм та ін.); несанкціонований доступ (підключення, зміна) до пристрою і інформаційно-програмного забезпечення (у тому числі базам даних); порушення фізичної цілісності ЦСК (окремих компонентів, пристроїв, обладнання, носіїв інформації); порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ЦСК (електроживлення, заземлення, охоронної сигналізації, вентиляція та ін.); порушення режимів функціонування ЦСК (обладнання і ПЗ); впровадження і застосування комп'ютерних вірусів, заставних (апаратних і програмних) пристроїв, інших засобів розвідки; впровадження і застосування ПЗ забороненого політикою безпеки або несанкціоноване використання ПЗ, за допомогою якого можна отримати доступ до критичної інформації (наприклад, аналізаторів безпеки мережі).</p>

#### 4 МОДЕЛЬ ПОРУШНИКА

4.1 Модель порушника - абстрактний неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії і ін. По відношенню до складових частин і ЦСК в цілому порушники можуть бути внутрішніми (з числа персоналу та користувачів системи) або зовнішніми (сторонні особи або будь-які особи, які знаходяться за межами контрольованої зони).

4.2 В ЦСК та його складових частинах потенційно можливими є наступні зовнішні і внутрішні джерела суб'єктивної природи (далі - порушники) ненавмисних і навмисних загроз:

- навмисні дії (спроби) потенційних зовнішніх і внутрішніх порушників під час експлуатації обладнання і технічних засобів компонентів ЦСК;
- ненавмисні дії (помилки) персоналу (внутрішні порушники) ЦСК під час експлуатації оснащення і технічних засобів компонентів ЦСК.

4.3 Метою навмисних дій зовнішніх і внутрішніх порушників можуть бути:

- спричинення збитків власнику і користувачам ЦСК шляхом знищення матеріальних і інформаційних цінностей;
- отримання необхідної інформації в потрібному об'ємі і складі;
- отримання можливості вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами).

4.4 Класифікація зовнішніх і внутрішніх порушників виконана на основі наступних критеріїв:

а) за рівнями можливостей, які надаються їм засобами складових частин ЦСК. Рівні є ієрархічними, тобто кожний наступний рівень включає функціональні можливості попередніх рівнів:

- 1) перший рівень - визначається можливістю ведення діалогу і можливістю запуску фіксованого набору задач (програм), які реалізують наперед передбачені функції обробки інформації;
- 2) другий рівень - визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- 3) третій рівень - визначається можливістю управління функціонуванням складових частин ЦСК, тобто впливом на базове програмне забезпечення системи і на склад та конфігурацію його обладнання;
- 4) четвертий рівень - визначається повним об'ємом можливостей осіб, які здійснюють проектування, реалізацію, впровадження, супровід програмно-апаратного забезпечення ЦСК, аж до включення в склад ЦСК власних засобів з новими функціями обробки інформації.

б) за рівнем знань про ЦСК:

- 1) володіють інформацією про функціональні особливості ЦСК, основні закономірності формування в ній масивів даних і потоків запитів до них, уміють користуватися штатними засобами;
- 2) володіють високим рівнем знань і досвідом роботи з технічними засобами ЦСК та з їх обслуговування;
- 3) володіють високим рівнем знань в області обчислювальної техніки і програмування, проектування і експлуатації ЦСК;
- 4) володіють інформацією про функції і механізми дії засобів захисту.

в) за методами і способами порушень, що використовуються:

- 1) використовують виключно агентурні методи отримання відомостей;
- 2) використовують пасивні технічні засоби перехоплення інформаційних сигналів;
- 3) використовують виключно штатні засоби ЦСК або недоліки проектування КСЗІ для реалізації спроб НСД;
- 4) використовують способи і засоби активного впливу на ЦСК, які змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ і т. ін.).

г) за місцем здійснення дії:

- 1) без отримання доступу на контрольовану територію ЦСК;
- 2) з отриманням доступу на контрольовану територію, але без доступу до технічних засобів ЦСК;

- 3) з отриманням доступу до робочих місць кінцевих (у тому числі віддаленого) користувачів ЦСК;
- 4) з отриманням доступу до місць накопичення і зберігання даних (баз даних, архівів, робочих станцій відповідних адміністраторів, серверів і т. ін.);
- 5) з отриманням доступу до засобів адміністрування і засобів управління КСЗІ складових частин ЦСК.

4.5 Відповідно до класифікаційних критеріїв в основу моделі зовнішніх порушників покладені наступні припущення:

1) кваліфікація (рівень знань) порушників:

- володіють високим рівнем знань в області обчислювальної техніки і програмування, проектування і експлуатації автоматизованих систем;
- володіють інформацією про функції і механізми дії засобів захисту операційних систем, мережних протоколів і СУБД, які використовуються в ЦСК;
- володіють високим рівнем знань і досвідом роботи з технічними засобами ЦСК і їх обслуговування;
- не володіють інформацією про функціональні особливості ЦСК, основні закономірності формування в ньому масивів даних і потоків запитів до них.

2) по рівню можливостей, які надаються їм засобами ЦСК:

- можливість запуску фіксованого набору задач (програм), які реалізують наперед передбачені функції обробки інформації;
- можливість створення і запуску власних програм з новими функціями обробки інформації;
- можливість управління функціонуванням складових частин ЦСК, тобто впливом на базове програмне забезпечення системи і на склад та конфігурацію його обладнання.

3) порушники використовують:

- агентурні методи отримання відомостей;
- пасивні технічні засоби перехоплення інформаційних сигналів;
- способи і засоби активного впливу на компоненти складових частин ЦСК, які змінюють конфігурацію системи (підключення до каналів передачі даних, впровадження і використання спеціального ПЗ і т. ін.);

4) порушники мають можливість реалізувати в складових частинах і ЦСК в цілому по каналах несанкціонованого отримання інформації (КНОІ) наступні класи загроз КНОІ - 1, 2, 4, 5 і 6 (див. таблицю 2).

5) порушники мають можливість реалізувати в складових частинах і ЦСК в цілому по каналах несанкціонованого порушення цілісності або доступності інформації (КНЦД) наступні класи загроз КНЦД - 1,2, 4, 5 і 6 (див. таблицю 3).

4.6 Відносно об'єктів ЦСК зовнішніми порушниками можуть бути наступні джерела суб'єктивної природи навмисних загроз, які розташовані в порядку убутання ступеня небезпеки:

1) злочинна діяльність окремих осіб, яка направлена на протизаконне отримання інформації або ресурсів, з метою нанесення збитків фізичним чи юридичним особам або досягнення матеріальної вигоди;

2) міжнародні системи передачі інформації (глобальні мережі);

3) національні і корпоративні системи передачі інформації, які знаходяться під управлінням інших операторів, і послуги яких надаються користувачам ЦСК;

4) діяльність суб'єктів підприємницької діяльності, окремих фізичних осіб, що направлена на отримання переваг в конкуренції.

4.7 В складових частинах і ЦСК в цілому внутрішні порушники можуть бути з наступних категорій осіб:

- користувачі, яким надані повноваження забезпечувати управління ЛОМ і ЦСК в цілому (адміністратори ЦСК);
- користувачі, яким надані повноваження розробляти і супроводжувати КСЗІ (адміністратор безпеки, керівник СЗІ ЦСК);

- віддалені користувачі (у тому числі взаємодіючих систем користувачів ЦСК), яким надано право доступу до конфіденційної інформації і критичної інформації ЦСК;
- звичайні користувачі (абоненти мереж загального користування), яким надано право доступу тільки до відкритої інформації;
- технічний обслуговуючий персонал, який забезпечує належні умови функціонування технічних засобів складових частин ЦСК;
- розробники і проектувальники апаратних засобів складових частин ЦСК, які забезпечують його модернізацію і розвиток;
- розробники прикладного програмного забезпечення, які здійснюють розробку і впровадження нових функціональних процесів, а також супровід вже діючих;
- постачальники обладнання і технічних засобів ЛОМ ЦСК і фахівці, які здійснюють їх монтаж, поточне гарантійне і післягарантійне обслуговування;
- технічний персонал, який здійснює повсякденну підтримку життєдіяльності фізичного середовища ЛОМ ЦСК (електрики, технічний персонал з обслуговування будівель, ліній зв'язку і т. ін.).

4.8 Відповідно до класифікаційних критеріїв в основу моделі внутрішніх порушників покладені наступні припущення:

#### 4.8.1 Рівень знань (кваліфікація)

Внутрішні порушники мають наступний рівень знань (кваліфікацію) про складові частини і ЦСК в цілому:

##### 1) адміністратори ЦСК, адміністратор безпеки, керівник СЗІ ЦСК:

- володіють інформацією про функціональні особливості ЦСК, основні закономірності формування в ній масивів даних і потоків запитів до них, вміють користуватися штатними засобами;
- володіють високим рівнем знань і досвідом роботи з технічними засобами ЦСК і їх обслуговування;
- володіють інформацією про функції і механізми дії засобів захисту.

##### 2) виділені і звичайні користувачі:

- володіють інформацією про функціональні особливості ЦСК, основні закономірності формування в ній масивів даних і потоків запитів до них, уміють користуватися штатними засобами;

##### 3) розробники і проектувальники апаратних засобів складових частин ЦСК і розробники прикладного ПЗ:

- володіють інформацією про функціональні особливості ЦСК, основні закономірності формування в ній масивів даних і потоків запитів до них, вміють користуватися штатними засобами;
- володіють високим рівнем знань і досвідом роботи з технічними засобами ЦСК і з їх обслуговування;
- володіють високим рівнем знань в області обчислювальної техніки і програмування, проектування і експлуатації автоматизованих систем;
- володіють інформацією про функції і механізми дії засобів захисту.

##### 4) технічний обслуговуючий персонал складових частин ЦСК :

- володіє інформацією про функціональні особливості ЦСК;
- володіє високим рівнем знань і досвідом роботи з технічними засобами ЦСК і з їх обслуговування;

##### 5) постачальники обладнання і технічних засобів ЛОМ ЦСК і фахівці, які здійснюють їх монтаж, поточне гарантійне і післягарантійне обслуговування:

- володіють високим рівнем знань в області обчислювальної техніки і експлуатації автоматизованих систем;

##### 6) технічний персонал, який здійснює повсякденну підтримку життєдіяльності фізичного середовища ЦСК (електрики, технічний персонал з обслуговування будівель, ліній зв'язку і т. ін.).

- не володіють достатнім рівнем знань в області обчислювальної техніки і експлуатації автоматизованих систем.

#### 4.8.2 Рівні можливостей.

Внутрішні порушники мають наступні рівні можливостей, які надаються їм засобами складових частин і ЦСК в цілому:

1) адміністратори ЦСК, адміністратор безпеки, керівник СЗІ ЦСК:

- мають можливості для управління функціонуванням складових частин і ЦСК в цілому.

2) віддалені і звичайні користувачі:

- мають можливість для запуску фіксованого набору задач (програм), які реалізують наперед передбачені функції обробки інформації.

3) розробники і проектувальники апаратних засобів складових частин ЦСК і розробники прикладного ПЗ:

- володіють повним об'ємом можливостей осіб, які здійснюють проектування, реалізацію, впровадження, супровід програмно-апаратного забезпечення ЦСК, аж до включення в склад ЦСК власних засобів з новими функціями обробки інформації.

4) технічний обслуговуючий персонал складових частин ЦСК, постачальники обладнання і технічних засобів ЦСК і фахівці, які здійснюють його монтаж, поточне гарантійне і післягарантійне обслуговування:

- володіють об'ємом можливостей осіб, які здійснюють впровадження, супровід програмно-апаратного забезпечення ЦСК, аж до включення в склад ЦСК власних засобів з новими функціями обробки інформації.

5) технічний персонал, який здійснює повсякденну підтримку життєдіяльності фізичного середовища ЦСК (електрики, технічний персонал з обслуговування будівель, ліній зв'язку і т. ін.):

- не володіють можливістю роботи з апаратними і програмними засобами складових частин ЦСК.

#### 4.8.3 Методи і способи порушень.

Внутрішні порушники можуть використовувати наступні методи і способи порушень:

1) адміністратори ЦСК, адміністратор безпеки, керівник СЗІ ЦСК можуть використовувати:

- агентурні методи отримання відомостей;
- штатні засоби ЦСК або недоліки проектування КСЗІ для реалізації спроб НСД;
- способи і засоби активного впливу на ЦСК, для несанкціонованої зміни конфігурації складових частин системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ та ін.).

2) виділені і звичайні користувачі можуть використовувати:

- агентурні методи отримання відомостей;
- штатні засоби ЦСК або недоліки проектування КСЗІ для реалізації спроб НСД;
- способи і засоби активного впливу на ЦСК, для несанкціонованої зміни конфігурації складових частин системи (модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ та ін.).

3) розробники і проектувальники апаратних засобів складових частин ЦСК і розробники прикладного ПЗ можуть використовувати:

- агентурні методи отримання відомостей;
- штатні засоби ЦСК або недоліки проектування КСЗІ для реалізації спроб НСД;
- способи і засоби активного впливу на ЦСК, для несанкціонованої зміни конфігурації складових частин системи (модифікація штатних технічних засобів, впровадження і використання спеціального ПЗ та ін.).

4) технічний обслуговуючий персонал складових частин ЦСК може використовувати:

- агентурні методи отримання відомостей;
- пасивні технічні засоби перехоплення інформаційних сигналів;
- штатні засоби ЦСК або недоліки проектування КСЗІ для реалізації спроб НСД;
- способи і засоби активного впливу на ЦСК, для несанкціонованої зміни конфігурації складових частин системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ та ін.).

5) постачальники обладнання і технічних засобів ЦСК і фахівці, які здійснюють його монтаж, поточне гарантійне і післягарантійне обслуговування можуть використовувати:

- агентурні методи отримання відомостей;
- пасивні технічні засоби перехоплення інформаційних сигналів;
- штатні засоби ЦСК або недоліки проектування КСЗІ для реалізації спроб НСД;
- способи і засоби активного впливу на ЦСК, для несанкціонованої зміни конфігурації складових частин системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ та ін.).

6) технічний персонал, який здійснює повсякденну підтримку життєдіяльності фізичного середовища ЛОМ ЦСК (електрики, технічний персонал з обслуговування будівель, ліній зв'язку і т. ін.) може використовувати:

- агентурні методи отримання відомостей;
- пасивні технічні засоби перехоплення інформаційних сигналів.

#### 4.8.4 Місце дії.

Внутрішні порушники можуть здійснювати ненавмисні і навмисні дії:

1) адміністратори ЦСК, адміністратор безпеки, керівник СЗІ ЦСК:

- з отриманням доступу до робочих місць кінцевих (у тому числі віддаленого) користувачів ЦСК;
- з отриманням доступу до місць накопичення і зберігання даних (баз даних, архівів, робочих станцій відповідних адміністраторів і т. ін.);
- з отриманням доступу до засобів адміністрування і засобів управління КСЗІ складових частин ЦСК.

2) виділені і звичайні користувачі:

- з отриманням доступу до робочих місць кінцевих (у тому числі віддаленого) користувачів ЦСК;
- з отриманням доступу до місць накопичення і зберігання даних (баз даних, архівів, робочих станцій відповідних адміністраторів і т. ін.).

3) розробники і проектувальники апаратних засобів складових частин ЦСК і розробники прикладного ПЗ:

- з отриманням доступу до робочих місць кінцевих (у тому числі віддаленого) користувачів ЦСК;
- з отриманням доступу до місць накопичення і зберігання даних (баз даних, архівів, робочих станцій відповідних адміністраторів та ін.);
- з отриманням доступу до засобів адміністрування і засобів управління КСЗІ складових частин ЦСК.

4) технічний обслуговуючий персонал складових частин ЦСК, постачальники обладнання і технічних засобів ЦСК і фахівці, які здійснюють їх монтаж, поточне гарантійне і післягарантійне обслуговування:

- з отриманням доступу до робочих місць кінцевих (у тому числі віддаленого) користувачів ЦСК;
- з отриманням доступу до місць накопичення і зберігання даних (баз даних, архівів, робочих станцій відповідних адміністраторів та інш.).

5) технічний персонал, який здійснює повсякденну підтримку життєдіяльності фізичного середовища ЦСК (електрики, технічний персонал з обслуговування будівель, ліній зв'язку і т. ін.):

- з отриманням доступу на контрольовану територію, але без доступу до технічних засобів ЦСК.

#### 4.8.5 Характер дій.

1) внутрішні порушники мають можливість реалізувати в складових частинах і ЦСК в цілому по каналах несанкціонованого отримання інформації (КНОІ) наступні класи загроз - 3, 4, 5 і 6 (див. таблицю 2), за винятком порушників зі складу технічного персоналу, які можуть реалізувати КНОІ 1-го і 2-го класів.

2) внутрішні порушники мають нагоду реалізувати в складових частинах і ЦСК в цілому по каналах потенційно можливих причин несанкціонованого порушення цілісності або доступності інформації (КНЦД) наступні класи загроз - 3, 4, 5 і 6 (див. таблицю 3), за винятком порушників зі складу технічного персоналу, які можуть реалізувати КНЦД 1-го і 2-го класів.

4.9 Результати класифікації внутрішніх порушників в складових частинах ЦСК з врахуванням висловлених припущень наведені в таблиці 4.

Таблиця 4. Класифікація внутрішніх порушників в складових частинах ЦСК

Групи внутрішніх порушників	Критерії класифікації															
	Рівні можливостей				Рівні знань про ЦСК				Методи і способи порушень, що використовуються				Місце здійснення дії			
Виділені і звичайні користувачі	+				+				+	+	+	+			+	+
Адміністр. ОС, СУБД, мережевого обладнання, сервісів та ін.				+	+	+		+	+	+	+	+			+	+
Адміністратор безпеки, керівник СЗІ ЦСК				+	+	+		+	+	+	+	+			+	+
Технічний обслуговуючий персонал				+	+	+			+	+	+	+			+	+
Розробники і проектувальники апаратних засобів				+	+	+	+	+	+	+	+	+			+	+
Розробники прикладного ПЗ		+		+	+	+	+	+	+	+	+	+			+	+
Постачальники обладнання і технічних засобів				+			+		+	+	+	+			+	+
Технічний персонал									+	+				+		

Примітка. \* можливості визначені для розробників апаратних засобів і прикладного ПЗ ЦСК.

4.10 Як впливає з приведеної класифікації внутрішні порушники в складових частинах ЦСК по можливості реалізації загроз конфіденційності інформації розташовуються в наступному порядку зменшення ступені небезпеки:

- виділені користувачі (у тому числі взаємодіючих систем клієнтів ЦСК і інших відомств), яким надано право доступу до конфіденційної інформації і критичної інформації;
- адміністратори ЦСК, адміністратор безпеки, керівник СЗІ ЦСК;



- розробники прикладного програмного забезпечення, які здійснюють розробку і впровадження нових функціональних процесів, а також супровід вже діючих;
- розробники і проектувальники апаратних засобів складових частин ЦСК, які забезпечують його модернізацію і розвиток;
- технічний обслуговуючий персонал, який забезпечує належні умови функціонування технічних засобів складових частин ЦСК;
- звичайні користувачі (абоненти мереж загального користування), яким надано право доступу тільки до відкритої інформації;
- постачальники обладнання і технічних засобів ЦСК і фахівці, які здійснюють його монтаж, поточне гарантійне і післягарантійне обслуговування;
- технічний персонал, який здійснює повсякденну підтримку життєдіяльності фізичного середовища ЦСК (електрики, технічний персонал з обслуговування будівель, ліній зв'язку і т. ін.).

4.11 По можливості реалізації загроз цілісності і доступності інформації і інформаційних ресурсів ЦСК внутрішні порушники в складових частинах системи розташовуються в наступному порядку зменшення ступеня небезпеки:

- розробники прикладного програмного забезпечення, які здійснюють розробку і впровадження нових функціональних процесів, а також супровід вже діючих;
- розробники і проектувальники апаратних засобів складових частин ЦСК, які забезпечують його модернізацію і розвиток;
- адміністратори ЦСК, адміністратор безпеки, керівник СЗІ ЦСК;
- технічний обслуговуючий персонал, який забезпечує належні умови функціонування технічних засобів складових частин ЦСК;
- виділені користувачі (у тому числі взаємодіючих систем ДП "ЕНЕРГОРИНОК" і інших відомств), яким надано право доступу до конфіденційної інформації різних класифікаційних рівнів і критичної інформації;
- звичайні користувачі (у тому числі взаємодіючих систем ДП "ЕНЕРГОРИНОК" і інших відомств), яким надано право доступу тільки до відкритої інформації;
- постачальники обладнання і технічних засобів ЛОМ ЦСК і фахівці, які здійснюють їх монтаж, поточне гарантійне і післягарантійне обслуговування;
- технічний персонал, який здійснює повсякденну підтримку життєдіяльності фізичного середовища ЦСК (електрики, технічний персонал з обслуговування будівель, ліній зв'язку і т. ін.).

## 5 ПЕРЕЛІК СУТТЄВИХ ЗАГРОЗ В ЦСК

5.1 За наслідками аналізу класифікаційних груп можливі загрози конфіденційності, цілісності і доступності інформації в кожній складовій частині локальної обчислювальної мережі ЦСК можна зробити наступні висновки.

5.1.1 На рівні окремих апаратно-програмних засобів складових частин ЦСК (системний блок ПЕОМ, принтер, дисплей, модем, абонентна лінія, операційна система, файл, каталог, база даних та ін.) суттєвими є наступні загрози:

- несанкціонований доступ (використання, підключення, зміна) до пристроїв і інформаційно-програмного забезпечення (у тому числі базам даних);
- перехоплення побічних електромагнітних випромінювань і наведень від пристроїв;
- неправомірна зміна режимів роботи пристроїв (окремого компонента, обладнання, ПЗ та ін.);
- несанкціоноване отримання інформації з обмеженим доступом (ІзОД);
- зчитування залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;
- несанкціоноване порушення фізичної і логічної цілісності ІзОД (знищення, модифікація), у тому числі за рахунок наявності вірусів, апаратних і програмних закладок в пристроях закордонного виробництва;
- розкрадання носіїв з ІзОД або копіювання інформації;
- порушення фізичної цілісності окремих компонентів пристроїв, обладнання, носіїв інформації;
- відмова (повний вихід з ладу) обладнання;
- неправильне виконання функцій (збій, помилки) обладнання.

5.1.2 Додатково до перерахованих загроз, на рівні локальної обчислювальної мережі ЦСК суттєвими є наступні загрози:

- несанкціонована зміна конфігурації (виключення штатних і/або підключення додаткових апаратно-програмних компонентів) ЛОМ;
- навмисне виведення з ладу елементів ЦСК (обладнання ЛОМ, каналоутворюючої апаратури та ін.);
- порушення функціонування компонента ЛОМ (у тому числі за рахунок наявності вірусів, апаратних і програмних закладок і ін.);
- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ЦСК (електроживлення, заземлення, охоронної сигналізації, вентиляції і ін.);
- отримання атрибутів доступу до ЛОМ з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад");
- впровадження і застосування ПЗ забороненого політикою безпеки або несанкціоноване використання ПЗ, за допомогою якого можна отримати доступ до критичної інформації (наприклад, аналізаторів безпеки мережі).

5.1.3 На рівні телекомунікаційних мережі ЦСК в цілому додатково до перерахованих загроз суттєвими є наступні:

- нав'язування користувачам помилкової інформації (у тому числі службової) при віддаленому доступі;
- порушення зв'язку за рахунок порушення каналу (тракту) передачі, атак на протоколи мережі, телекомунікаційні служби, нав'язування помилкової службової інформації і режимів роботи в системі управління, як окремих мереж, так і ЦСК в цілому, включаючи зміну маршруту передачі інформації та ін.;
- маскування під зареєстрованого користувача або запити системи;
- видача одного суб'єкту за іншого з метою використання його повноважень для формування помилкової інформації;
- видача одного об'єкту або суб'єкту за іншого, для того, щоб зняти з себе відповідальність за реалізовані (або спроби реалізувати) певні загрози;
- відмова одержувача (відправника) від факту прийому (передачі) інформації або твердження, що вона прийнята (передана) в інший час;
- формування одержувачем помилкової інформації, нібито отриманої від відправника;
- твердження відправника про те, що повідомлення або запит передавалися, хоча насправді вони не передавалися або передавалися в інший час;
- твердження одержувача тому, що повідомлення або запит отримано від певного користувача, хоча насправді вони сформовані одержувачем (порушником);

- навмисна зміна одержувачем повідомлень з метою порушення їх цілісності і автентичності;
- формування відправником помилкового підтвердження отримання інформації, нібито прийнятого від одержувача;
- несанкціонована зміна особистих повноважень або повноважень інших користувачів на відправлення і отримання повідомлень;
- зараження вірусами по інформаційних і службових каналах мережі зв'язку та ін.

## 6 СПОСОБИ ЗДІЙСНЕННЯ ЗАГРОЗ

6.1 Опис можливих технічних каналів витоку інформації.

6.1.1 Загроза витоку ІзОД залежно від форми існування може здійснюватися по технічних каналах побічних електромагнітних випромінювань і наведень (ПЕМВН).

6.1.2 Витік ІзОД при обробці на технічних засобах може здійснюватися по каналах побічних електромагнітних випромінювань і наведень за рахунок:

- перехоплення за межами КЗ інформативних випромінювань ПЕОМ при обробці ІзОД у спеціальних приміщеннях;
- наведень інформативних сигналів ПЕОМ у спеціальних приміщеннях на елементи незахищених ДТЗС, які мають вихід за межі КЗ.

6.1.3 В перерахованих можливих технічних каналах витоку інформації можуть використовуватися:

- портативні засоби технічної розвідки;
- апаратні та програмні закладні пристрої.

6.1.4 Оцінка можливості реалізації технічних каналів витоку інформації.

6.1.4.1. Оцінка можливості реалізації каналів побічних електромагнітних випромінювань і наведень

Аналіз складу ОТЗ і ДТЗС, просторового розміщення об'єкту, віддалення об'єктів від меж контрольованої території, технічних характеристик засобів технічної розвідки дозволяє зробити висновки, що на об'єкті ЦСК можливі загрози:

- витоку інформації по каналах ПЕМВН за рахунок перехоплення за межами КЗ інформативних випромінювань ПЕОМ при обробці ІзОД у спеціальних приміщеннях;
- витоку інформації по каналу ПЕМВН за рахунок наведень інформативних сигналів ПЕОМ у спеціальних приміщеннях на елементи незахищених ДТЗС, які мають вихід за межі КЗ.

При зміні схеми розташування приміщень ЦСК або складу ОТЗ повинна бути виконана повторна оцінка.

6.2 Канали спеціального впливу.

6.2.1 Оцінка можливості реалізації каналів спеціального впливу проводиться для технічних засобів електронної обчислювальної техніки, телекомунікаційного обладнання і інформаційно-телекомунікаційних каналів об'єктів ЦСК.

6.2.2 Оцінка проводиться шляхом аналізу складу і технічних характеристик обладнання, умов прокладки і підключення кабелів ліній зв'язку, територіального розміщення і віддалення об'єктів від меж контрольованої території, характеристик систем електроживлення (включаючи підключення до фідерів і місцеположення трансформаторних підстанцій).

6.2.3 Беручи до уваги характеристики і умови застосування технічних засобів силового електромагнітного впливу (ТЗ СЕВ), можна зробити висновок, що реалізація каналів спеціального впливу на зовнішні інформаційно-телекомунікаційні канали ЦСК можлива, але маловірогідна. Це обумовлено тим, що ТЗ СЕВ не є засобами селективного впливу і наносять руйнування не тільки конкретному об'єкту нападу, але і іншому обладнанню і апаратурі, що підключені до фідера електроживлення або кабелю лінії зв'язку, по якому здійснюється напад на об'єкт. Іншими словами дії ТЗ СЕВ можуть бути спрямовані на всю апаратуру і обладнання будинків, де розташовані ЛОМ ЦСК.

## **7 ОЦІНКА ПЕРЕДБАЧУВАНОВОГО ЗБИТКУ У РАЗІ РЕАЛІЗАЦІЇ ЗАГРОЗ**

7.1 Єдина методика розрахунку вартості збитку, нанесеного власнику і користувачам ЦСК внаслідок реалізації загроз ІзОД, критичній інформації і ресурсам системи, відсутня. Це зв'язано з тим, що інформація може бути викрадена або знищена (змінена) частково або повністю. Можуть бути виведені з ладу тимчасово (постійно), частково (повністю) ресурси ЦСК. Втрати інформації мають ситуативну і довготривалу вартість. Вартість втрат інформації залежить від ефективності її використання порушником, а також від сфери використання інформації - політичної, економічної та ін.

7.2 В загальному випадку компоненти вартості збитку визначаються експертним шляхом, при підсумовуванні використовуються вагові коефіцієнти. Отже, при оцінці збитку розглядаються різні комбінації еквівалентів втрат інформації.

## 8 ШЛЯХИ РЕАЛІЗАЦІЇ ОСНОВНИХ ЗАГРОЗ ТА СПОСОБИ ЇХ НЕЙТРАЛІЗАЦІЇ

8.1 У таблиці 5 наведені загрози безпеки інформації й шляхи їх реалізації в ЦСК при його функціонуванні.

Таблиця 5 - Загрози (при автоматизованій обробці)

Загроза	Атака	Час проведення атаки	Об'єкт атаки (місце-положення)	Суб'єкт атаки (місцеположення )	Код загрози
Модифікація інформації	Зміна ПЗ	Поза процесом функціонування системи	Будь-яка РС ЛОМ	Ця ж РС ЛОМ	I1
				Будь-яка РС ЛОМ → Сервер	
			Сервер взаємодії	Сервер взаємодії	
			Сервер	Будь-яка РС ЛОМ	
		Сервер	3 будь-якої РС ЛОМ		
	Неправильне введення	В процесі функціонування системи	Будь-яка РС ЛОМ	Ця ж РС ЛОМ	I2
				Будь-яка РС ЛОМ → Сервер	
	Впровадження програмної закладки	В процесі функціонування системи	Будь-яка РС ЛОМ	Ця ж РС ЛОМ	I3
				Будь-яка РС ЛОМ → Сервер	
			Сервер взаємодії	Сервер взаємодії	
Сервер				Будь-яка РС ЛОМ	
Перехоплення	В процесі функціонування системи	Сервер	Будь-яка РС ЛОМ	I4	
		В процесі передачі даних	Мережа передачі даних	Проміжні вузли	I5
Модем	Проміжні вузли				
Введення неіснуючої інформації	Зміна ПЗ	Поза процесом функціонування системи	Будь-яка станція ЛОМ	Ця ж РС ЛОМ	I1
				Будь-яка РС ЛОМ → Сервер	
			Сервер зв'язку	Сервер взаємодії	
				Сервер	
	Впровадження програмної закладки	В процесі функціонування системи	Будь-яка станція ЛОМ	Ця ж РС ЛОМ	I3
				Будь-яка РС ЛОМ → Сервер	
			Сервер зв'язку	Сервер зв'язку	
				Сервер	
	“Ручне введення”	В процесі функціонування системи	Сервер	Будь-яка РС ЛОМ	I6
			Сервер зв'язку	Сервер взаємодії	
			ЛОМ	Будь-яка РС ЛОМ	
		В процесі передачі даних	Мережа передачі даних	Проміжні вузли	I7
			Модем	Проміжні вузли	
Порушення конфіденційності	Зміна ПЗ	Аналогічно попередньому випадку			
	Впровадження програмної закладки	Аналогічно попередньому випадку			

Загроза	Атака	Час проведення атаки	Об'єкт атаки (місце-положення)	Суб'єкт атаки (місцеположення )	Код загрози
	Перегляд з екрану	В процесі функціонування системи	Будь-яка РС ЛОМ	Будь-яка РС ЛОМ	18
			Сервер взаємодії	Сервер взаємодії	
	Перехоплення	В процесі функціонування системи	ЛОМ	Будь-яка РС ЛОМ	14
			В процесі передачі даних	Мережа передачі даних	Проміжні вузли
		Модем			
	Несанкціоноване копіювання	Поза процесом функціонування системи	Сервер	Будь-яка РС ЛОМ	19
Відмова від факту отримання	Зміна ПЗ	В процесі функціонування системи	Будь-яка станція ЛОМ	Будь-яка РС ЛОМ	13
		В процесі передачі даних	Сервер зв'язку	Сервер взаємодії	
			Зовнішня організація	Зовнішня організація	
Відмова від авторства	Аналогічно попередньому випадку				
Дублювання	Зміна ПЗ	Аналогічно попередньому випадку			
	Впровадження програмної закладки	Аналогічно попередньому випадку			
	“Повтор в мережі”	В/поза процесом функціонування системи	Сервер	Будь-яка РС мережі	112
			ЛОМ	Будь-яка РС мережі	
			Мережа передачі даних	Проміжні вузли	
			Модем		
Втрата або знищення	Перехоплення	В процесі функціонування системи	Сервер	Будь-яка РС мережі	14
			ЛОМ	Будь-яка РС мережі	
			Мережа передачі даних	Проміжні вузли	
			Модем		
	Несанкціоноване копіювання	Поза процесом функціонування системи	Сервер	Будь-яка РС ЛОМ	19
	Зміна ПЗ	Аналогічно попередньому випадку			
	Впровадження програмної закладки	Аналогічно попередньому випадку			
НСД до РС	НСД	В/поза процесом функціонування системи	Будь-яка РС ЛОМ	Ця ж РС ЛОМ	113
				Будь-яка РС ЛОМ → Сервер	
			Сервер взаємодії	Сервер взаємодії	
			Сервер	Будь-яка РС ЛОМ	
			Будь-яка РС ЛОМ	Із зовнішньої мережі (Internet)	

Загроза	Атака	Час проведення атаки	Об'єкт атаки (місце-положення)	Суб'єкт атаки (місцеположення)	Код загрози
НСД до каналу передачі даних	НСД до каналу	В процесі функціонування системи	ЛОМ	Будь-яка РС мережі	I14
		В процесі передачі даних	Мережа передачі даних	Проміжний вузол	I15
			Модем		
Напад із зовнішньої мережі	Атака із зовнішньої мережі	В/поза процесом функціонування системи	Сервер		I18
			РС мережі		
			Модем		
			Маршрутизатор		
Порушення працездатності процесу функціонування системи	Змін ПЗ, зміна конфігурації апаратних засобів, впровадження програмних закладок	В/поза процесом функціонування системи	На всіх технологічних ділянках	На всіх технологічних ділянках	I17
Несанкціонована зміна конфігурації	Несанкціоновані зміни конфігурації	В/поза процесом функціонування системи	Сервер взаємодії	Будь-яка станція мережі передачі даних	I18

8.2 У таблиці 6 наведені заходи захисту від загроз, які характерні для ЦСК.

Таблиця 6 - Заходи захисту від загроз

Код загр.	Заходи захисту		
	Організаційні	Фізичні	Технічні
I1	Інструкції користувачам Встановлення відповідальності за порушення правил Визначення повноважень користувачів	Розмежування доступу в приміщення Фізичний захист приміщень	Завантаження РС з гнучких магнітних дисків Захист файлів, що виконуються, від зміни Замкнуте середовище дозволених для запуску програм для кожного користувача системи Періодичний контроль цілісності виконуваних файлів і налаштувань програмних засобів Використання ЕЦП Реєстрація подій
I2	Контроль проходження документів Інструкції користувачам Встановлення відповідальності за порушення правил	Ні	Контроль проходження документів (за допомогою ПЗ) Реєстрація подій
I3	Інструкція по внесенню змін в конфігурації ПЗ Інструкції користувачам Встановлення відповідальності за порушення правил	Розмежування доступу в приміщення Фізичний захист приміщень	Завантаження РС з гнучких магнітних дисків Захист виконуваних і системних файлів від зміни Замкнуте середовище дозволених для запуску програм для кожного користувача системи Періодичний контроль цілісності системи Реєстрація подій Використання засобів виявлення нападів
I4	Інструкція по внесенню змін в конфігурації ПЗ	Розмежування доступу в	Обмеження доступу до серверу по номеру мережевої карти



	Інструкції користувачам Завдання відповідальності за порушення правил Інструкція по зміні повноважень користувачів	приміщення Фізичний захист приміщень	Дозвіл доступу до серверу тільки із захищених робочих станцій Заборона одночасного доступу до серверу користувачів з однаковим ім'ям Захист серверів Реєстрація подій Використання засобів виявлення атак
I5	Договір із зовнішньою організацією	За рамками повноважень ЦСК	Перетворення інформації Використання ЕЦП Контроль часу
I6	Інструкція по зміні повноважень користувачів Інструкції користувачам Встановлення відповідальності за порушення правил	Ізоляція системи, що захищається, від інших систем ЦСК	Обмеження доступу до РС, серверу та ін. Дозвіл доступу до серверу тільки з захищених робочих станцій Обмеження доступу до серверу за номером мережевої карти Заборона одночасного доступу до серверу користувачів з однаковим ім'ям Реєстрація подій Використання засобів виявлення нападів
I7	Договір із зовнішньою організацією	За рамками повноважень ЦСК	Використання ЕЦП Перетворення інформації Контроль часу
I8	Інструкції користувачам Встановлення відповідальності за порушення правил	Розмежування доступу в приміщення Фізичний захист приміщень	Обмеження доступу до РС Розмежування доступу до РС
I9	Інструкції користувачам Встановлення відповідальності за порушення встановлених правил	Розмежування доступу в приміщення Фізичний захист приміщень	Обмеження доступу до серверів Дозвіл доступу до серверів тільки з визначених РС Заборона одночасного доступу до серверів користувачів з однаковим ім'ям Перетворення інформації Захист серверів Реєстрація подій Використання засобів виявлення нападів
I10	Договір із зовнішньою організацією Ведення архівів ЕЦП	За рамками повноважень ЦСК	Реєстрація подій Використання ЕЦП
I11	Інструкції користувачам Встановлення відповідальності за порушення встановлених правил	Ізоляція системи, що захищається, від інших систем	Обмеження доступу до РС Розмежування доступу до РС Реєстрація подій Використання засобів виявлення нападів
I12	Інструкції користувачам Встановлення відповідальності за порушення правил Ведення архівів ЕЦП	Ізоляція системи, що захищається, від інших систем	ЕЦП Контроль часу Реєстрація подій
I13	Інструкції користувачам Встановлення відповідальності за порушення правил Інструкція з використання систем захисту інформації від НСД Обмеження людей, що мають право конфігурувати ЦСК	Розмежування доступу в приміщення Фізичний захист приміщень Ізоляція системи, що захищається, від інших систем ЦСК	Обмеження доступу до РС, серверу Розмежування доступу користувачів до РС, серверу Реєстрація подій Зміна стандартного імені адміністратора системи захисту Дозвіл роботи в мережі тільки одного адміністратора безпеки Власником всіх файлів, які виконуються, в системі, а також критичних налаштувань повинен бути адміністратор безпеки Використання засобів виявлення нападів Використання міжмережевих екранів

			Використання антивірусних програм Використання всіх вбудованих засобів захисту
I14	Інструкції користувачам Встановлення відповідальності за порушення правил	Захист кабельної системи	-
I15	За рамками повноважень ЦСК		
I16	Інструкції користувачам Встановлення відповідальності за порушення правил	Розмежування доступу в приміщення Фізичний захист приміщень	Обмеження доступу до архіву Резервне копіювання Використання антивірусних програм
I17	Всі заходи	Всі заходи	Всі заходи
I18	Інструкції користувачам Встановлення відповідальності за порушення правил		Обмеження числа модемів, що використовуються Фізична ізоляція РС для доступу в глобальні мережі від РС системи Обмеження доступу до РС Реєстрація подій Використання засобів виявлення нападів Використання міжмережевих екранів Використання всіх вбудованих в систему засобів захисту

## 9 ВИСНОВКИ

9.1 В ЦСК існує можливість реалізації загроз конфіденційності, цілісності і доступності інформації шляхом несанкціонованого доступу.

9.2 В ЦСК при недотриманні вимог політики безпеки існує можливість витоку інформації по каналах побічних електромагнітних випромінювань і наведень від засобів обчислювальної техніки і телекомунікаційного обладнання при обробці ІзОД.

9.3 Реалізація каналів спеціального впливу на зовнішні інформаційно-телекомунікаційні канали ЦСК можлива, але маловірогідна.

9.4 Модель підлягає перегляду при зміні планів розміщення, умов функціонування і характеристик ЦСК.